UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/800,561	03/15/2004	Shoichi Awai	7217/71978	9794

530 7590 09/05/2006

LERNER, DAVID, LITTENBERG,
KRUMHOLZ & MENTLIK
600 SOUTH AVENUE WEST
WESTFIELD, NJ 07090

EXAMINER	
SANDERS, AARON J	

ART UNIT	PAPER NUMBER
2191	

DATE MAILED: 09/05/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/800,561	AWAI, SHOICHI	
	Examiner	Art Unit	
	Aaron J. Sanders	2191	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 March 2004* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Priority

Acknowledgment is made of applicant's claim for foreign priority based on an application filed in Japan on 3 April 2003. It is noted, however, that applicant has not filed a certified translation of the Japanese application as required by 35 U.S.C. 119(b).

Drawings

The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because the 'certificate server' in Fig. 2 is designated by reference character '70' in the specification, but in Fig. 2 it is designated by reference character '73'. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

The disclosure is objected to because of the following informalities: margins should be one inch. Appropriate correction is required.

The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 4 and 6 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 4 is rejected because the second clause is grammatically incomprehensible. For purposes of examination, the claim is interpreted to mean generally that updated digital data is stored back into the external storage means based on the results of a comparison to the backed up data. Appropriate correction is required.

Claim 6 is rejected because the sentence structure in the second part of the claim is incomprehensible and counterintuitive. For purposes of examination and based on the Applicant's specification, the claim is interpreted to read that 'an inquiry is made to the external certificate server'. Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-5 are rejected under 35 U.S.C. 102(b) as being anticipated by Yano et al., U.S. Pat. 6,711,594.

As per claims 1-5, Yano et al. teach:

1. A data service apparatus comprising:
storage means for storing digital data (See e.g. Brief Description par. 8, 'a reading/writing means for reading/writing digital data from/onto a portable recording medium');
an encryption circuit for encrypting digital data into encrypted data (See e.g. Brief Description par. 9, 'a means for encrypting data');
a decryption circuit for decrypting encrypted data into its initial digital data (See e.g. Brief Description par. 9, 'individual divided data are decrypted or, alternatively, to perform the decryption after the divided data are integrated'), and wherein
digital data, to be backed up, stored in the storage means is extracted, encrypted by the encryption circuit into encrypted data and stored in an external storage unit (See e.g. Fig. 3, S1 'medium reading and authentication', S23 'division/encryption', and S31 'divided file writing' where, see Brief Summary par. 8, 'the divided parts are each transferred to the plurality of servers on the network and are distributed/saved therein'); and
encrypted data, to be decrypted, stored in the external storage unit is extracted, decrypted by the decryption circuit into the initial digital data and written back to the storage means (See e.g. Fig. 3, S43 'reading of divided files that constitute the to-be-extracted file', S47 'decryption/integration of divided files', and S51 'saving of the to-be-extracted file' where, see Brief Summary par. 8, 'it becomes possible to access the saved data from an arbitrary distributed data archive device connected to the network as long as the portable recording medium is carried with the user').

2. The data service apparatus according to claim 1, further comprising an identification code generation circuit for generating an identification code unique to the data service apparatus (See e.g. Brief Summary par. 7, 'a data management means for recording... data-saving

procedure information that indicates a dividing method of the data to be saved and the like' which includes, see Detailed Description par. 10, 'A unique file name is designed to be given to each of the divided files formed on the basis of the to-be-saved data file in accordance with a predetermined rule') wherein

the encryption circuit performs the encryption according to the identification code generated by the identification code generation circuit (See e.g. Brief Summary par. 9, 'cryptographic key information and the like that are needed for encryption/decryption are recorded as the data-saving procedure information by the data management means'); and

the decryption circuit performs the decryption according to the identification code generated by the identification code generation circuit (See e.g. Brief Summary par. 9, 'cryptographic key information and the like that are needed for encryption/decryption are recorded as the data-saving procedure information by the data management means').

3. The data service apparatus according to claim 2, further comprising a falsification detection circuit for checking, when decrypting the digital data from the encrypted data, the digital data according to the identification code generated by the identification code generation circuit, and for inhibiting the initial digital data from being written back to the storage means when it is found that the digital data has been falsified (See e.g. Detailed Description par. 38, 'Since an IC card with very great security against illegal data falsification can be used as the archive card 10 needed when data is saved and when the data is extracted, there is no fear that saved data will be stolen', Detailed Description par. 20 , 'The authenticity of the distributed data archive device 1... is checked on the side of the archive card 10 while the authenticity of the archive card 10 is being checked by the verification means 12', and Fig. 3, S1 'medium reading and authentication' where, if the data is falsified, it is not read).

4. The data service apparatus according to any one of claims 1, 2 and 3, further comprising a comparison circuit for making a comparison in attribute data between the digital data in the storage means and the digital data stored in the external storage unit (See e.g. Detailed Description par. 9, 'Information (i.e., URL list of the data servers) that shows the data server on which each of the four divided files F11 to F14 is saved is stored onto the management folder of FIG. 2 as management data (data depository information) of the file F1' where an attribute of the data is the server's URL), wherein

digital data, updated after previously backed up in the external storage unit, stored in the storage means is stored into the external storage unit according to a comparison result from the comparison circuit (See e.g. Detailed Description par. 4, 'the data depository information is constructed by a list of addresses (i.e., Uniform Resource Locator, which is hereinafter referred to as URL) of a plurality of data servers that are depository destinations' where, see Detailed Description par. 38, the data can be updated because 'It is possible to very conveniently access the saved data from an arbitrary distributed data archive device connected to the network if the archive card 10 is carried').

5. The data service apparatus according to claim 4, further comprising:

a detection circuit for detecting an optimum file of digital data for storage as a file into the external storage unit (See e.g. Detailed Description par. 16, 'one divided file is constructed

with data in which one byte is taken at every third byte if three divided files are formed' where taking every third byte is 'optimal' because, see Detailed Description par. 16, 'it is preferable to prevent the contents of the original file from being perceived in the case where only one divided file has been read');

an aggregation circuit for aggregating a plurality of files into one file (See e.g. Brief Summary par. 7, 'an integration/reconstitution means for reconstituting divided/saved data into an original single data file');

a division circuit for dividing a file into a plurality of files each having a predetermined size (See e.g. Brief Summary par. 7, 'a division means for dividing data to be saved into a plurality of parts');

a synthesis circuit for combining the divided files together into one file (See e.g. Brief Summary par. 7, 'an integration/reconstitution means for reconstituting divided/saved data into an original single data file'); and

a separation circuit for separating one file formed from a plurality files into the plurality of files (See e.g. Brief Summary par. 7, 'a division means for dividing data to be saved into a plurality of parts'), wherein

for backup of the digital data:

digital data read by the aggregation circuit from the storage means are aggregated into one file (See e.g. Brief Summary par. 8, 'when the data to be saved is extracted, the data to be saved that has been distributed into the plurality of servers on the network and has been saved therein is extracted');

the file as a result of the aggregation is divided by the division circuit according to the size detected by the detection circuit (See e.g. Detailed Description par. 16, 'one divided file is constructed with data in which one byte is taken at every third byte if three divided files are formed'); and

the file as a result of the division being stored into the external storage unit (See e.g. Brief Summary par. 8, 'a network communication means for transferring the data files divided by a communication protocol determined among data servers keeping the data to be saved'); and wherein

for decryption of the digital data:

the encrypted data stored in the external storage unit are decrypted and combined by the synthesis circuit into an initial one file (See e.g. Brief Summary par. 9, 'the integration/reconstitution means reconstitutes the divided data into the original data in such a way as to perform the integration after the saved individual divided data are decrypted'); and

the file as a result of the synthetic combination is separated by the separation circuit into the plurality of initial digital data and written back to the storage means (See e.g. Fig. 3, S51 'saving of the to-be-extracted file' where the file is saved to the card, Fig. 1 where there can be more than one 'to-be-saved data file', and therefore after the files have been individually recombined from the data servers they are still separate from each other on the card and therefore a 'plurality of initial digital data and written back to the storage means').

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Yano et al. as applied to claims 1-5 above, and further in view of Murty et al., U.S. P.G. Pub. 2003/0084290.

6. The apparatus according to claim 5, further comprising a communications circuit for performing information communications with an external certificate server, wherein

an inquiry is made about whether the digital data to be decrypted may be restored to the external certificate server via the communications circuit, and the restoration is done only when the communications circuit has received a permission of restoration from the external certificate circuit (See e.g. Murty et al. [0029], 'To obtain the symmetric storage key, the HSED 22 must authenticate itself with the security appliance 20. This authentication may be achieved in any one of a number of different ways, but preferably involves the HSED 22 sending a certificate signing request to the security appliance 20' where Murty et al. [0028], 'the HSED 22 intercepts the incoming data and decrypts (using the symmetric storage key 26) what is read from the drive before delivering this information to the host server 12a').

Yano et al. do not explicitly disclose using a certificate server to authenticate the access rights of the portable storage medium, however Murty et al. do make such a disclosure. Yano et al. and Murty et al. are analogous art because they both discuss protecting digital files transferred over a network. At the time of the invention, it would have been obvious to one of ordinary skill in the art to use a certificate server for authentication. The motivation for this is found in Murty et al. [0009], where a certificate server is used 'to provide an improved post-side encryption module for encrypting data for storage on a storage area network, and for decrypting encrypted data received from the storage area network'.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aaron J. Sanders whose telephone number is 571-270-1016. The examiner can normally be reached on M-Th 7:30a-5:00p.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David Bruce can be reached on 571-272-2487. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AJS

DAVID BRUCE
SUPERVISORY PATENT EXAMINER